Statement of Work for
Enterprise Data Management
&
Engineering Division
Office of Information and Technology

Security & Technology Policy Branch Information Systems Security Officer (ISSO) Services Support

VERSION 4.0

HSBP1008J23882

September 2008

This page intentionally left blank

Table of Contents

Statement of Work (SOW)

1.0 PROJECT TITLE

CBP Office of Information and Technology Information Systems Security Officer Support (ISSO)

2.0 BACKGROUND

The Bureau of Customs and Border Protection (CBP), Office of Information and Technology (OIT), Enterprise Data Management & Engineering Division (EDME), Security and Technology Policy Branch (STP), is responsible for providing Certification and Accreditation (C&A) support to CBP and the Department of Homeland Security (DHS). This support includes, but is not limited to, the following:

- Certification and Accreditation (C&A) support for systems and applications.
- Risk assessments of CBP and select Department of Homeland Security (DHS) sites, as needed.
- Promoting DHS Sensitive System Policy Directives 4300A.
- Identifying and analyzing security risks and mitigation solutions.
- Governing and enforcing security policies.
- Developing CBP information system security policies, standards and procedures for Sensitive but Unclassified (SBU) systems.
- Liaison activities within CBP, the Department of Homeland Security, other government agencies including law enforcement agencies, the international trade community and private firms as they relate to security compliance issues, security programs, policies, issues and products.

DHS Chief Information Officer (CIO) has mandated 100 percent certification and accreditation of all DHS Major Applications (MA) and General Support Systems (GSS). The DHS Chief Information Security Officer (CISO) tracks each DHS component's C&A progress. In order to standardize the C&A effort throughout DHS, DHS has mandated the use of two software products: Risk Management System (RMS) and Trusted Agent FISMA (TAF). Only artifacts created using DHS mandated software shall be accepted for credit. STP works on a program-by-program basis, to assure all the systems security documentation and information is complete and ready for the CBP C&A process.

3.0 SCOPE OF WORK

The scope of this Statement of Work (SOW) encompasses contractor development of a program to provide enterprise-wide systems security support to STP, including, but not limited to; C&A, risk assessments and mitigation strategies, security policy and procedures, security architecture and Security Test and Evaluation.

The contractor shall be accountable for maintaining and reporting accurate and current technical, administrative and financial status of the IT security program, and other related activities. The contractor shall submit this information in periodic status reports described elsewhere in this document.

The contractor shall provide qualified technical and administrative support personnel who are well qualified and are willing to become familiar with the policy and regulations of CBP.

The Contractor shall be flexible and adjust accordingly to meet Government needs when changes occur, such as workload increases, realignments, reorganizations, etc.

4.0 SPECIFIC TASKS

4.1 TASK 1 - CERTIFICATION AND ACCREDITATION

The contractor shall provide technical security expertise in planning, coordinating, preparing and executing certification and accreditation support for Customs & Border Protection. In support of this task, the contractor shall ensure that CBP information systems and technology are secure and meet all applicable security requirements. In attaining this goal, the contractor shall support the Security & Technology Branch with the review and support of certification and accreditation documentation, participation in technical meetings, on-site observations, and efficient use of automated accreditation tools and preparation of technical papers. Each member of the C&A team shall serve as the Certification Agent (CA) and/or the Information Systems Security Officer (ISSO) for several systems, and SBU major applications and general support systems. However, the team member shall not serve as both the CA and the ISSO for the same Information system. Furthermore, in order to eliminate any conflict of interest, Government Leads shall serve as the Certifying Agents for any systems for which an STP contractor serves as the ISSO. All artifacts in support of the C&A must meet Federal, DHS and CBP requirements.

4.1.1 Information Systems Security Officer (ISSO)

The contractor shall provide personnel to perform ISSO duties in support of the C&A process at CBP. The ISSO shall be a point of contact in STP to provide security solutions and interpretations of security policies as they relate to specific security infrastructure, architectures and information systems (IS's). The ISSO shall establish rapport and develop a relationship with the system development team(s) to become a recognized and integral

member of the team. An ISSO shall typically serve in that role for more than one project. The ISSO shall perform duties including but not limited to:

- Participate in appropriate actions to certify and accredit each IS.
- Notify the ISSM through Point of Contact (POC) when an assigned system requires accreditation or re-accreditation.
- Assist in the certification and accreditation of each system.
- Provide policy and technical advice to systems designers, implementers and operators.
- Conduct risk assessments and prepare an appropriate summary of findings for inclusion within the accreditation documentation.
- Conduct self-assessments of the CBP major applications and general support systems, which shall include vulnerabilities identified at contractor/consultant facilities.
- Recommend corrective actions for deficiencies found during system self assessments (NIST 800-26 or NIST 800-53A) reviews and or during any review or monitoring period for the system/application.
- Ensure timely Plan of Action & Milestones (POA&Ms) is uploaded and updated in the Trusted Agent FISMA tool as required.
- Develop draft, review and endorse all information systems security plans and other C&A artifacts, not including the Security Assessment Report (SAR). These artifacts include but are not limited to the development of the following documents:
  - Privacy Threshold Determination
  - Privacy Impact Assessment (PIA)
  - E-Authentication Determination
  - Controls Testing (Security Test and Evaluation (ST&E)) Plan
  - ST&E Plan Test Results
  - Authorization to Operate (ATO) Authorization Letter
  - Self Assessment (National Institute of Standards and Technology Special Publication (NIST SP 800-53) Guide for Information Security Program Assessments and System Reporting Form
  - Standards for Security Categorization of Federal Information and Information Systems (FIPS 199) Assessment
  - Risk Assessment
  - System Security Plan
  - Contingency Plan
  - Contingency Plan Test and Test Results
  - Security Test & Evaluation (ST&E)
  - Security Assessment Report
  - Plans of Actions & Milestones (POA&Ms)
- At the request of CSIRC, assist in the investigation of security violations and incidents.
- Be knowledgeable on current Federal, National, DHS and CBP standards, policies, requirements and procedures.

- Complete/update a NIST SP 800-26 or NIST SP 800-53 review for each major application, LAN(s), or general support system on a yearly basis.
- Review and Update System Security Plan annually and when significant security changes occur.

4.2 TASK 2 - COMMUNICATIONS SECURITY (COMSEC)

COMSEC is the system of security measures used to protect classified information or material utilizing cryptographic keying material and equipment. COMSEC measures are taken to deny unauthorized personnel information derived from telecommunications of the U.S. Government concerning national security and to ensure the authenticity of such telecommunications. COMSEC includes cryptography, transmissions security and physical security of communications security material and information. Currently CBP utilizes the services DHS COMSEC Office of Record (COR). In the future CBP may opt to recreate its own centralized COMSEC COR.

4.2.1 COMSEC Custodian

The contractor shall serve as COMSEC Custodians for accounts specified by the Chief, STP Branch. The contractor shall perform COMSEC Custodian duties including but not limited to:

- Receipt, custody, issuance, safeguarding, accounting for and when necessary, destruction of COMSEC material for offices and/or operating units under their areas of responsibility.
- Maintaining up-to-date records of COMSEC inventory and submitting required accounting reports.
- Administering initial briefing and debriefing to individual users.
- Maintain copies of all briefings and debriefings.
- Undergo required COMSEC training within six months of appointment and update training yearly.
- Programming and local distribution of COMSEC devices such as the Secure Telephone Equipment (STE) and QSEC 2700, a secure cell phone.
- Receipt, loading and management of COMSEC keying material using devices such as the Electronic Key Management System (EKMS), Data Transfer Device (DTD), Simple Key Loader (SKL) and Secure DTD-2000 System (SDS).

4.2.2 COMSEC Office of Record (COR)

The contractor shall provide COMSEC COR services related to the distribution, governance and maintenance of keying material, secure phones and other COMSEC equipment. The contractor shall perform duties including but not limited to:

- Manage and perform centralized COMSEC accounting functions for CBP.

- Provide keying material for CBP with the use of EKMS.
- Perform NSA required audits of each COMSEC account in CBP every 18 months to ensure compliance with NSA and DHS policies.
- Provide COMSEC Custodian and COMSEC equipment training.
- Provide a Help Desk for technical and administrative questions.
- Evaluate new COMSEC equipment and fax machines for use by CBP.
- Represent CBP on Intelligence Community and National Security Agency Policy Working Groups and Committees.
- Provide Controlling Authority function for all CBP COMSEC keying material.
- Appoint new COMSEC Custodians.
- Set up new COMSEC accounts.
- Support COMSEC users on the set up of new secure communications circuits to meet mission needs.
- Provide assistance visits to CBP COMSEC accounts.
- Manage centralized maintenance contracts for COMSEC equipment.
- Maintain a pool of COMSEC equipment, to provide immediate replacement of operational equipment for use in establishing emergency circuits and to replace equipment in need of repair.
- Maintain visibility of all COMSEC assets in CBP to allow cross leveling of equipment or to direct a transfer of excess equipment to meet operational requirements.
- Coordinate and manage centralized Memorandum of Agreement (MOA) and funding for Defense Courier Services (DCS) support.
- Provide technical support to CBP to facilitate interoperability of purchases of COMSEC equipment.
- Provide a central Point of Contact (POC) for secure phone service with vendors such as T-Mobile, Verizon and ATT.
- Provide centralized support service for Satellite phone equipment and service.
- Advocate CBP issues with NSA and the Intelligence Community, to ensure the CBP perspective is heard in operational and policy forums.
- Complete documents and updates to databases as required by DHS 4300B, National Security Systems Handbook. The documentation includes but is not limited to: COMSEC account information, COMSEC Custodian training documentation, COMSEC Facilities documentation, COMSEC Material Accounting, and, COMSEC Incident Reports.

4.3 TASK 3 - COMPUTER FORENSICS SPECIALIST

The contractor shall provide Computer Forensics services related to the recovery of evidence of illegal activities conducted via computer such as computer system intrusion (hacking). The contractor shall perform duties including but not limited to:

- Research, evaluate and recommend computer forensic techniques, hardware and software

- Assist in gathering and organizing of electronic evidence
- Document receipt and release of evidence and transfer case files from Lab to long-term storage
- Disassemble, configure and troubleshoot computer hardware, including cell phones and PDAs
- Perform various computer forensic techniques to gain access to digital evidence and make it available to CBP staff and CBP Officers
- Maintain detailed written work logs and case documentation following forensic procedures;
- Able to testify on computer forensic activities

4.4 TASK 4 - TECHNOLOGY POLICY ADMINISTRATION – SECTION 508

Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to and use of information and services that is comparable to the access and use available to non-disabled Federal employees and members of the public.

The contractor shall perform the following duties on a case by case basic to include but not limited to:

- Assist the CBP Section 508 Coordinator in proper implementation of Section 508 Law.
- Ensure CBP policies adhere to Section 508 Law.
- Provide expert advice and assistance to CBP Program Offices to ensure major applications and general support systems adhere to Section 508 Law.
- Perform Section 508 Training to CBP personnel.

All deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following standards have been identified:

- 36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as Flash or Asynchronous JavaScript and XML (AJAX) then "1194.21 Software" standards apply to fulfill functional performance criteria.
- 36 CFR 1194.31 – Functional Performance Criteria applies to all deliverables regardless of delivery method. All deliverable shall use technical standards,

regardless of technology, to fulfill the functional performance criteria.

- 36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required "1194.31 Functional Performance Criteria", they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

- 36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards.

  When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.
- 36 CFR 1194.3(b) – Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.
- 36 CFR 1194.3(f) – Back Office, applies to any EIT item that will be located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment. This exception does not include remote user interfaces that are accessible outside the enclosed "space".

4.5 TASK 5 - SECURITY RISK ASSESSMENT

STP is tasked to conduct Security Risk Assessments (SRAs) of its Local Area Network

(LAN) systems throughout the United States and the world, as needed. The number of trips scheduled to perform the SRAs should be considerably less since sites in close proximity are assessed in a single trip. In order to assess the overarching security posture of CBP field sites, a sample of CBP field locations are visited in order to identify the likelihood of threats occurring, the controls in place to prevent or minimize exploitation of the vulnerabilities found, and the severity of the impact on the CBP mission of a threat exploiting identified vulnerabilities. The SRA and Report are based on guidance from NIST SP 800-30, NIST SP 800-26 and NIST SP 800-53 Self Assessment Questionnaire. The contractor shall perform risk assessments to support such CBP functional areas that require connection to the CBP network.

The contractor shall review a sampling of the following types of CBP field LAN sites:

- Office of Field Operations (OFO) port offices, cargo inspection areas, field offices, airports, and pre-clearance sites;
- OIT field laboratories;
- OIT LANs in the Washington, DC metropolitan area;
- Office of Air and Marine branch offices;
- Office of Border Patrol branch locations;
- Office of International Affairs Container Security Initiative (CSI) sites; and
- Any other DHS component sites as they migrate to the CBP network.

The contractor shall perform duties including but not limited to:

- Support audits by providing information dealing with LAN risk assessments and related methodology.
- Schedule risk assessments based on importance of the site's mission, type of site (e.g., CSI, Pre-Clearance, Border Patrol branch office, ICE, airport, cargo inspection areas, port offices, laboratories, cargo inspection areas, field offices, Air and Marine branch offices, field offices), geographic area of site location (i.e., sampling of sites from each region and system, and size of site (i.e., number of terminals supported by the LAN at the site).
- Plan and coordinate site visit with the field office (i.e., notify them of the planned visit, collect and review all available information and data available at the site (e.g. LAN Continuity of Operations Plan, Physical Security Assessment Report, Floor Plan, Organization Plan, Mission Statement and artifacts from any prior Security Risk Assessment).
- Coordinate network vulnerability scans with the Computer Security Incident Response Center (CSIRC) and review the scans for high-risk network vulnerabilities.
- Perform a physical inspection of the site and minimally interview the LAN administrator, site management, and system users using documented interview questions.
- For each LAN site SRA characterize the organization and mission, identify supporting assets, identify threats, identify existing security controls and

vulnerabilities, and map to controls and vulnerabilities to those recommended by NIST SP 800-53 guidance.

- From the data collected from the pre-assessment phase of the SRA, physical inspections, and interviews; determine likelihood of identified threat occurrences, severity of impact on the CBP mission if vulnerability is exploited, and associated risk ratings. Develop recommendations regarding mitigation strategies for all identified vulnerabilities.
- Within one month of the SRA at the CBP LAN sites, deliver the Security Risk Assessment Report documenting a description of the mission performed at the locations visited, pertinent physical characteristics of the site and its security posture including supporting assets, threats, vulnerabilities, security controls identified.
- Populate a Plan of Action and Milestones (POA&M) table with the significant vulnerabilities identified by each SRA. Capture this information in the SRA database used to track the progress of the remediation.
- Plan and organize monthly POA&M meetings with the organizations that manage each type of site both from a functional and IT perspective.
- At these POA&M meetings, determine and plan the risk mitigation strategies and/or levels of acceptable risk, establish milestones and estimate the time to mitigation/resolution of vulnerabilities.
- Continually track and update milestones until resolution of the vulnerabilities. Include the information in the SRA database and in TAF, the DHS tool. Update TAF on a monthly basis with any changes in status.

4.6 TASK 6 - SECURITY TEST AND EVALUATION

- The contractor shall perform Security Testing and Evaluation of a select number of the CBP General Support Systems and applications in support of their Certification and Accreditation and continued improvements to the CBP security posture.
- Personnel must have technical expertise in performing security evaluations of all
- CBP major applications, Operating Systems and network Internet Operating System (IOS). This includes but is not limited to: Microsoft, Solaris and Linux
- Operating System, Mainframe (Z/OS), Oracle database, Cisco for wired and wireless Local Area Networks (LANs) and Wide Area Networks (WANS).
- Personnel must perform the testing and document the significant findings in the Security Test and Evaluation report. The documentation must include summary of findings, impact of finding, and recommendations for fixes or other security mitigation strategies.

4.7 TASK 7 - GENERAL TASKS

4.7.1 Compliance Measurement

As documented in the Customs Information Systems Handbook (CIS HB) 1400-05B, CBP Security Policy and Procedures Handbook, and as part of CMM process improvement, the

contractor shall assist in the development of metrics appropriate to measure the compliance and state of the CBP security posture and the effectiveness of the audit, assessment and documentation implementation and compliance.

4.7.2 EA (Enterprise Architecture) Compliance

- HLS EA Clause – Developed Solutions: (include following descriptions of developed solutions)

  All developed solutions shall be compliant with the HLS EA.

- HLS EA Clause – Hardware/Software: (include following descriptions of developed hardware/software)

  All IT hardware or software shall comply with the HLS EA.

- HLS EA Compliance for Data:

  All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.

- IPv6 Clause

  In compliance with OMB mandates, all network hardware provided under the scope of this Statement of Work and associated Task Orders shall be IPv6 compatible without modification, upgrade, or replacement.

4.7.3 Communications Plan

The contractor shall develop a plan that includes tailored delivery of the CBP security message while establishing the expectation for compliance and the consequences for noncompliance. The communications plan shall be the vehicle to deliver the security message as it relates to areas such as: policy and procedures, architecture, training and incident identification and reporting. The contractor shall utilize all available means to communicate the necessary information, to include: conferences, conference calls, meetings, committees and incorporation into performance evaluation.

4.7.4 Key Personnel

The Contractor agrees to assign to the task order: Sr. Security IT Specialist are technically qualified to support and fill the necessary requirements of the task order, whose resumes are submitted with its proposal, and who are specifically defined as key personnel. No substitutions shall be made except in accordance with this clause

The Contractor shall not make any personnel changes of Key Personnel unless an individual's sudden illness, death, or termination of employment necessitates such substitution. In case of these occurrences, the Contractor shall notify the Contracting Officer promptly and submit documentation pertaining to the proposed substitution in writing at least (30) calendar days in advance of the proposed substitution.

The Contractor must provide a detailed explanation of the circumstance necessitating the proposed substitution. a complete resume for each proposed substitute and any other information requested by the Contracting Officer, to permit evaluation of the impact on the program. All resumes submitted for each proposed substitution must have qualifications that are equal to or superior to the qualifications of the person being substituted to perform the work under this task order.

The Contracting Officer and COTR shall evaluate the resume of each requests and promptly notify the Contractor whether the proposed substitution has been approved or disapproved. No diversion shall be made by the Contractor without the written consent of the Contracting Officer: provided, that the Contracting Officer may confirm in writing such diversion and such confirmation shall constitute the consent of the Contracting Officer dictated by this clause.

5.0 DELIVERABLES

All deliverables produced as a result of this SOW shall become the property of the Government.

5.1 DELIVERABLE REQUIREMENTS

A Deliverable Document Plan will be required 30 days after task order award. The Deliverable Document Plan will be delivered in both draft and final version to the government. The draft version will be delivered to the COTR to accept or discuss changes. A final Deliverable Document Plan would be due to COTR 15 days after acceptance of the draft version.

Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date
Security Assessment Reports	4.1.1	As Required	As Required
Privacy Impact Assessment (PIA)	4.1.1	As Required	As Required
E-Authentication	4.1.1	As Required	As Required

Controls Testing (Security Test and Evaluation (ST&E)) Plan and Results	4.1.1	As Required	As Required
Authorization to Operate (ATO) Letter	4.1.1	As Required	As Required
Self Assessment (NIST SP 800-26, 800-53A)	4.1.1	As Required	As Required
FIPS-199 Assessment	4.1.1	As Required	As Required
Risk Assessment	4.1.1	As Required	As Required
System Security Plan	4.1.1	As Required	As Required
Contingency Plan	4.1.1	As Required	As Required
Contingency Plan Test Results	4.1.1	As Required	As Required
C&A Artifacts and documentation as specified by DHS and/or CBP requirements	4.1	As Required	As Required
Maintain detailed written work logs and case documentation following forensic procedures	4.3	As Required	As Required

Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date
Technology Policy Administration – Section 508 • Assist the CBP Section 508 Coordinator in proper implementation of Section 508 Law. • Ensure CBP policies adhere to Section 508 Law. • Provide expert advice and assistance to CBP Program Offices to ensure major applications and general support systems adhere to Section 508 Law	4.4	As Required	As Required
Risk Assessment Security Questionnaire	4.5	As Required	As Required

Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date
Risk Assessment Site Visit Plan and Process Documentation	4.5	As Required	As Required
Controls Testing (Security Test and Evaluation (ST&E)) Plan and Results	4.5	As Required	As Required
Risk Assessment Report	4.5	As Required	As Required
Plans of Action and Milestones Documents	4.5	As Required	As Required
Security Test and Evaluation Report	4.6	As Required	As Required
Communications Plans	4.7.2	As Required	As Required
Weekly Status Report with an overview of work accomplished the previous period and work scheduled for the upcoming week. Other information required includes personnel leave, travel, training, etc. These reports will be deemed accepted upon delivery. This report can be changed at the discretion of the COTR and will be defined upon the outset of this award.	5.2.2	Weekly	Weekly
Monthly Status Report shall address work completed during the current period, planned activities, which should include leave schedules, request for upcoming travel, problems/issues with recommended solutions, anticipated delays, and resources expended.	5.2.3	Monthly	Monthly
Cost Report	5.2.4	Monthly	Monthly
Ad Hoc Reports, such as, but not limited to: • Trip reports; • Meeting agenda reports; • Meeting minutes; • Other reports required by the COTR	5.2	As Required	As Required

Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date
Kick-Off Meeting/Draft Project Schedule • The contractor shall provide a draft schedule of their plan to meet the customer's requirements as identified in this statement of work.	7.1	Ten Workdays after Award	Ten Workdays after Award
The contractor shall submit within ten (10) working days after award a list containing the full name, social security number, and date of birth of those people who shall require background investigation by CBP, and submit such information and documentation as may be required by the Government to have a BI performed	9.0	Ten Workdays after Award	Ten Workdays after Award

5.2 REPORTS

All reports shall be delivered in softcopy electronic format. Softcopies shall be delivered utilizing Microsoft Office file formats. The Contractor shall submit all reports electronically to the COTR's DHS-CBP electronic mail address. In the event the system is unavailable or not accessible due to a system malfunction, the Contractor shall submit all reports in a typewritten format to be followed simultaneously with an electronically transmitted copy as soon as the electronic mail system becomes available.

Deliverable format shall be based on the type of document and shall conform to CBP directives, where appropriate, and be consistent with other similar efforts. Deliverables shall be accurate in presentation, technical content and adherence to accepted elements of style. In addition, deliverables shall be clear and concise; with engineering terms and project management tools used, where appropriate. All graphics shall be easy to understand, properly labeled with legends and be relevant to the supporting narrative.
Deliverables must conform to the On-Site Technical Manager(s) (OTM(s)) (i.e., Government Team Leads that oversee the project, resources, resource planning, project scope) specifications.

The contractor shall provide the COTR and OTM with a copy of all report deliverables furnished under this task order in soft copy via e-mail.

5.2.1 Status Reports

Report to address work completed during the current period, planned activities for the next period and any related problems or issues

5.2.2 Weekly Reports

The written weekly report shall consist of a summary of significant events and actions accomplished for the week. A bi-weekly verbal presentation shall consist of the following: actions accomplished for the previous two-week period; actions planned; and any issues of concern that may require special attention. This verbal report shall be presented to the Chief, STP Branch, COTR, and the OTMs on the second and fourth Thursday or as otherwise scheduled by the COTR.

5.2.3 Monthly Report

The contractor shall submit monthly status reports to the COTR and OTMs on progress made during the respective reporting period in performance of the work requirement. The reports shall address work completed during the current period, planned activities, which should include leave schedules, request for upcoming travel, problems/issues with recommended solutions, anticipated delays, and resources expended. The reports shall be sufficiently detailed to provide an ongoing record of all support efforts.

These reports shall be submitted within 5 calendar days following the end of each work month. (Each work month is defined as 30 consecutive calendar days.) The monthly report shall be delivered in hard copy to the COTR and OTMs. One electronically provided (i.e., via email) soft copy shall be sent to the COTR. The report shall be in a format to be agreed upon with the COTR.

5.2.4 Cost Reports/Invoices

To ensure the timely processing of the contractor's invoices, the contractor shall provide the COTR with copies of timesheets at the end of each timesheet period for each person with hours expended in support of the contract over the reporting period.
Invoices shall contain the following information:

- Date invoice is issued;
- Contract number;
- Period of performance (start and expiration date);
- Funding Source (e.g., Base, CSI, COBRA, and ACS Life Support), which shall be identified to the contractor upon award of the task order.
- For each funding source and task area listed, the contract labor categories and the names of the persons associated with the labor category;
- Contract labor category rate;
- Straight time labor hours by person (regular/extended time [i.e., no overtime charges may be submitted; just straight time] over the period of performance;
- Cumulative straight time labor hours by person (regular/extended time) for contract period of performance;

- Labor sub-totals for each funding category and task area;
- Travel and per diem charges by person for invoice period (with receipts for expenses incurred) and cumulative over the contract period.
- Employee Timecards – upon request

Invoices shall include Grand Totals for all funding sources, labor categories, and travel for the contract. The next pages of the report shall contain the following fields:
Period of performance expiration date, Hours-the number of hours billed against the contract for that month; Cost – this is the amount billed against the contract for that month; Allocated - this is the award amount of the contract (i.e., this is the amount the Government obligated to the contract); Cumulative - this is the amount billed against the contract since the beginning of the contract; PCT - This the percentage billed to date, remaining – This is the amount remaining on the task assuming that month's invoice is approved to date.

The invoice shall contain the following statement signed and dated by an authorized company representative: "This is to certify that the services set forth herein were performed during the period stated."

5.2.5 Invoice Submission

The vendor shall invoice the Government monthly for services performed under the contract. Invoices shall be for services and travel incurred against the contract during the previous month's period of performance. The period of performance shall begin on the first of the month and end on the last day of that month. Invoices shall be received by the tenth day of each month and include billable items for the previous month's period of performance. One (1) copy of the invoice document shall be submitted to the COTR at the following address:

Bureau of Customs and Border Protection
7451 Boston Boulevard, (b)(6), (b)(7)(C)
Springfield, Virginia 22153
Attn: (b) (6)

One (1) copy of the invoice shall be submitted to:
cbpinvoices@dhs.gov

Simultaneously, one copy of the invoice shall be mailed to the Contracting Officer at the following address:

Bureau of Customs and Border Protection
Office of Finance, Procurement
Attn: (b) (6), Contract Specialist
1300 Pennsylvania Avenue, NW
Washington, DC 20229

5.2.6 Invoice Modification

The contractor shall endeavor to ensure that all employee timesheet submissions and all travel receipts are accurate and valid, and as such, the invoices submitted to the Government should not require future changes. In the event that an error is made, the change shall be recorded and invoiced within ninety (90) days of the last day of the month in which the labor or travel was performed. In addition, any such adjustment shall contain detailed documentation explaining the error and the time period during which it occurred. No changes shall be accepted after ninety (90) days of the end of the period of performance.

At the COTR's discretion, the format of the invoice may be changed. The COTR shall notify the contractor of the change in format at least 60 days prior to requiring its use by the contractor.

5.3 TRAVEL / ODC

All travel shall be in accordance with the Federal Travel Regulations (for travel in 48 contiguous states), the Joint Travel Regulations, DoD Civilian Personnel, Volume 2, Appendix A (for travel to Alaska, Hawaii, Puerto Rico, and U.S. territories and possessions), and the Standardized Regulations (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" (for travel not covered in the Federal Travel Regulations or Joint Travel Regulations). Travel expenses shall be separately identified on invoices accompanied by all paid receipts during the time of travel. Travel will be reimbursed in accordance with applicable accounting procedures, the Federal Travel Regulations and the Federal Acquisition Regulation (FAR 31.205-46) only upon prior travel authorization by the COTR or the designated Task Monitor.

The contractor shall acquire the COTR or his/her designee's approval on all travel prior to initiating any Travel plans. No contractor personnel will perform travel unless specifically approved by the COTR, or the designated Task Monitor.

NOTE: Travel is the ONLY authorized ODC

6.0 GOVERNMENT FURNISHED INFORMATION AND EQUIPMENT

6.1 GOVERNMENT FURNISHED EQUIPMENT

CBP will provide, for all contractor Government-site personnel, on-site facilities to perform any work required under this task order The Government-site facilities will consist of a desk, chair, telephone, computer equipment with LAN/WAN interface, document file cabinets, access to copiers and fax machines and consumable supplies for personnel working directly on this contract. All work shall occur on government provided

equipment. The Contractor will be provided access to Government information as needed in the performance of the task.

6.2 GOVERNMENT FURNISHED INFORMATION

- Customs Directive No. 51715-006 Separation Procedures for Contractor Employees (CF-242);
- CBP Information Systems Security Policies and Procedures Handbook (HB 1400-05C) to be furnished upon award;
- CBP Process Asset Library (PAL);
- CBP Technical Reference Model (TRM);
- Current CBP enterprise architecture documentation;
- CBP Network, Directory, Messaging, Collaboration, and Engineering Documentation.

6.3 USE OF GOVERNMENT OWNED VEHICLES

In the performance of this cost-reimbursement task order requirement, the Contractor shall have access, if available, to Government Owned Vehicles for the sole purpose of official government-approved TDY or local travel. The Government will be responsible for maintaining the vehicles and providing the proper inventory of this property. The Contractor shall provide and maintain motor vehicle liability insurance covering bodily injury and property damage, in the amounts of $200,000 per person and $500,000 per occurrence for bodily injury and $20,000 per occurrence for property damage, protecting the Contractor and the Government against third-party claims arising from the ownership, maintenance, or use of an interagency fleet management system vehicle (IFMS).

The Contractor shall establish and enforce suitable penalties for their employees who use or authorize the use of Government vehicles for other than performance of work under this task order (see 41 CFR 101-38.301-1), subject to review and approval of the COTR. The Contractor shall assume without the right of reimbursement from the Government, the cost or expense of any use of interagency fleet management vehicles (IFMS) and services not related to the performance of the contract.

7.0 BRIEFINGS AND MEETINGS

Each briefing/meeting shall cover the essential elements of the relevant subject matter and shall be prepared and presented in a clear, concise, and orderly manner. Appropriate briefing tools such as Microsoft PowerPoint, overhead slides, plotted charts, etc., shall be used. Hardcopy handouts of all briefing materials shall be made available to all attendees prior to, or at the time of, the briefing.

7.1 MEETINGS

Kick-Off Meeting/Draft Project Schedule – A task order kick-off shall be scheduled within 10 days after award. Attendees shall be at a minimum: CBP COTR, On-Site Technical Managers (OTMs), Contracting Officer, Program Manager and contractor. The contractor shall provide a draft schedule of their plan to meet the customer's requirements as identified in this statement of work. This shall be due within 10 workdays after award of the task order. Any changes or adjustments to this schedule shall be coordinated with the appropriate OTM.

Periodic Meetings: CBP will coordinate periodic meetings and reviews to ensure all relevant provisions of the task order are being met.

8.0 PERFORMANCE

The contractor shall follow the performance guidelines listed below.

8.1 PLACE OF PERFORMANCE

The Government will provide access to appropriate resources within the DHS-CBP facilities, including, but not limited to: related employees/ vendors/ developers/ consultants, appropriate work space, hardware, software, network connections, test and live data. Support of this task may also require travel to various CBP locations throughout the United States.

All CBP Field Support Region locations in the Washington, D.C. Metropolitan area and locations within a 50-mile radius of the D.C. metro area at the discretion of the COTR, Current regional locations are listed below;

- NORTHEAST REGION
  Customs and Border Protection
  1 Penn Plaza, 10th Floor
  New York, NY 10119

  Customs and Border Protection
  220 Chestnut St. Room 1006
  Philadelphia, PA 19106

- SOUTHEAST REGION
  Customs and Border Protection
  1900 Lakemont Ave
  Orlando, FL 32803

- CENTRAL REGION
  Customs and Border Protection
  610 South Canal St, 3rd Floor
  Chicago, IL 60607

- SOUTHWEST REGION
  Customs and Border Protection
  3600 E Paisano Blvd, Bldg D
  El Paso, TX 79905

  Customs and Border Protection
  207 W Del Mar Ave
  Laredo, TX 78041

- NORTHWEST REGION
  Customs and Border Protection
  1000 2nd Ave
  Seattle, WA 98104

  FAR WEST REGION;
  Customs and Border Protection
  3752 Beyer Blvd #20
  San Ysidro, CA 91977

  Customs and Border Protection
  2430 South Swan Road
  Tucson, AZ 85711

NOTE: The current Regional location are subject to change at anytime, locations are subject to space availability within the regions.

8.2 HOURS OF OPERATIONS

All work shall be performed during a normal 40-hour week -- Monday through Friday, with core hours from 9:00 AM until 3:00 PM. Core hours refer to the hours of the day contractors shall work. The contractors shall come to work no later than 9:00AM. The contractor can start earlier than 9:00 AM but shall not end their day earlier than 3:00PM. Contractors shall take at least 30 minutes for lunch. For example, a contractor must spend 8 hours and 30 minutes at work to claim an 8-hour day.

Contractor personnel may not work more than 40 hours a week without prior approval from the COTR. Approved overtime hours shall be invoiced at the normal hourly rate.

The contractor staff shall observe the following government holidays unless the COTR approves otherwise:

New Year's Day,
Martin Luther King's Birthday,
Presidents' Day,
Memorial Day,
Independence Day,
Labor Day
Columbus Day
Veterans Day
Thanksgiving Day
Christmas Day

Any other day designated by Federal statute, by Executive Order or by the President's proclamation.

When any such day falls on a Saturday the preceding Friday is observed. When any such day falls on a Sunday, the following Monday is observed. Observance of such days by

Government personnel shall not be cause for an extension to the delivery schedule or period of performance or adjustment to the price, except as set forth in the task order.

Except for designated around-the-clock or emergency operations, contractor personnel will not, without written consent from the COTR, be able to perform on site under this task order with CBP on the holidays set forth above. Contractor will not charge any holiday as a direct charge to the task order. In the event that Contractor personnel work during a holiday other than those above, no form of holiday or other premium compensation will be reimbursed as either a direct or indirect cost. However, this does not preclude reimbursement for authorized overtime work.

In the event CBP grants administrative leave to its Government employees, at the site, on-site Contractor personnel shall also be dismissed if the site is being closed, however, Contractor shall continue to provide sufficient personnel to perform around-the-clock requirements of critical efforts already in progress or scheduled and shall be guided by the instructions issued by the CO or her/his duly appointed representative. In each instance when the site is closed to Contractor personnel as a result of inclement weather, potentially hazardous conditions, explosions, or other special circumstances; Contractor shall direct its staff as necessary to take actions such as reporting to its own site(s) or taking appropriate leave consistent with its policies. The cost of salaries and wages to Contractor for the period of any such site closure are a reimbursable item of direct cost under the task order for employees whose regular time is normally a direct charge if they continue to perform SOW work; otherwise, costs incurred because of site closure are reimbursable as indirect costs in accordance with the Contractor's established accounting policy.

Work may only be performed on a Federal holiday and/or at the Contractor's site with written consent of the COTR.

Assigned Task Monitors (TM's) will have the authority (delegated by the COTR) to approve requests for deviations from the defined work schedule (to include overtime hours billed as noted below). Requests for deviations from the defined work schedule must be submitted for prior approval in writing (e-mail preferred) by the contractor's team member to their TM. TM's will provide e-mail notification of approved requests to the COTR and contractors Project Manager. Urgent verbal requests and approvals must be subsequently documented in writing. Billing rates for overtime work will be the same as the standard billing rate for the individual under this contract. (However, for individuals classified as non-exempt under the Fair Labor Standards Act, billing rates for hours worked in excess of 40 hours a week will be one-and-a-half times the standard billing rate for the individual under this contract).

8.3 CONTRACTOR EMPLOYEE CONDUCT

Contractor shall be responsible for maintaining satisfactory standards of employee competency conduct appearance and integrity and shall be responsible for their employee's performance or the quality of their services. At the outset of the award, the Contractor and

COTR shall develop and institute a tasking procedure for traceability.

8.4 ADDITIONAL TASK ORDER OR PERSONNEL REQUIREMENTS

Contractor shall ensure that its employees will identify themselves as employees of their respective company while working on CBP tasks. For example, Contractor personnel shall introduce themselves and sign attendance logs as employees of their respective companies, not as CBP employees.

Contractor shall ensure that their personnel use the following format signature on all official e-mails generated by CBP computers:

[Name]
[Position or Professional Title]
[Company Name]
Supporting the XXX Division/Office…
US Customs and Border Protection
[Phone]
[FAX]
[Other task order information as desired]

8.5 NON-DISCLOSURE OF INFORMATION

Any information made available to Contractor by the Government shall be used only for the purpose of carrying out the provisions of this task and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the task. Contractor will be requested to sign Non-Disclosure statements.

8.6 PERIOD OF PERFORMANCE

The maximum term of each action including all options will be for five years. The new Task Order will consist of a base period of one year starting on September 30, 2008 thru September 29, 2009. Option Year 1, Option Year 2, Option Year 3, and Option Year 4 each will be for one year as displayed in the following chart:

	Base	Option 1	Option 2	Option 3	Option 4
Period of Performance	09/30/2008 thru 09/29/09	09/30/09 thru 09/29/10	09/30/10 thru 09/29/11	09/30/11 thru 09/29/12	09/30/12 thru 09/29/13

8.6.1 Government Estimated Staff Requirements

The following table reflects the government's estimated staff requirements within designated labor categories to perform the requirements set forth within this SOW. In addition to these requirements, at the Government's option, any or all of the following additional Level of Effort labor requirements may be ordered. The below listed optional requirements apply to the base period as well as all optional periods. *This additional level of effort requirements may be invoked one at a time (individually), in combinations, or in total during base period or any optional periods depending on need and funding availability. These items should be priced by each discrete unit.*

Base LOE – 09/30/08 – 09/29/09

Base 12 Months Period of Performance 09/30/08 - 09/29/098		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	9	17280
		0
		0
		0
TOTAL	9	17280

Optional LOE for BASE

Base 12 Months -optional Period of Performance 09/30/08 - 09/29/098		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	14	26880
		0
		0
		0
TOTAL	14	26880

Total possible LOE for Base Year if all estimated hours are required by the Government: Not To Exceed (NTE) 44,160 hours.

Option Year 1 LOE – 09/30/09 – 09/29/10

Option Year 1 Period of Performance 09/30/09 -09/29/10		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	9	17280
		0
		0
		0
TOTAL:	9	17280

Optional LOE for Option Year 1

Option Year 1 Period of Performance 09/30/09 -09/29/10		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	20	38400
IT Security Specialist	3	5760
		0
		0
		0
TOTAL:	23	44160

Total possible LOE for Option Year 1 if all estimated hours are required by the Government: NTE 61,440 hours.

Option Year 2 LOE –09/30/10 – 09/29/11

Option Year 2 Period of Performance 09/30/10-09/29/11		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	9	17280
		0
		0
		0
TOTAL:	9	17280

Optional LOE for Option Year 2

Option Year 2 Period of Performance 09/30/10-09/29/11		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	25	48000
IT Security Specialist	3	5760
		0
		0
		0
TOTAL:	28	53760

Total possible LOE for Option Year 2 if all estimated hours are required by the Government: NTE 71,040 hours.

Option Year 3 LOE – 09/30/11 – 09/29/12

Option Year 3 Period of Performance 09/30/11-09/29/12		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	9	17280
		0
		0
		0
		0
TOTAL:	9	17280

Optional LOE for Option Year 3

Option Year 3 Period of Performance 09/30/11-09/29/12		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	30	57600
IT Security Specialist	3	5760
		0
		0
		0
TOTAL:	33	63360

Total possible LOE for Option Year 3 if all estimated hours are required by the Government: NTE 80,640 hours.

Option Year LOE 4 – 09/30/12 – 09/29/13

Option Year 4 Period of Performance 09/30/12 – 09/29/13		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	9	17280
		0
		0
		0
TOTAL:	9	17280

Optional LOE for Option Year 4

Option Year 4 Period of Performance 09/30/12 – 09/29/13		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
Sr. Security IT Specialist	37	71040
IT Security Specialist	3	5760
		0
		0
		0
TOTAL:	40	76800

Total possible LOE for Option Year 4 if all estimated hours are required by the Government: NTE 94,080 hours.

This is a CPFF type contract. Over the term of this contract, the Government may incrementally fund and increase the LOE, if required, up to the Not to Exceed Ceiling.

TOTAL Possible LOE if all Optional Positions and Hours are required		
LABOR CATEGORIES	NUMBER OF POSITIONS	TOTAL HOURS
BASE + Optional LOE	23	44,160
Option Year 1 + Optional LOE	32	61,440
Option Year 2 + Optional LOE	37	71,040
Option Year 3 + Optional LOE	42	80,640
Option Year 4+ Optional LOE	49	94,080
TOTAL:	183	351,360

8.7 ACCEPTANCE REQUIREMENTS

The on-site technical manager (OTM) shall review all deliverables for accuracy and completeness. The contractor shall make those corrections required by the OTM. The deliverables require acceptance by the appropriate OTM or the COTR.

8.7.1 General Acceptance Criteria

Specific criteria shall be set forth for each task area, if applicable. Accordingly, general quality measures, as set forth below shall be applied to each work product received from the contractor under this SOW.

Accuracy - Work products shall be accurate in presentation, technical content and adherence to accepted elements of style.

Clarity - Work products shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand and be relevant to the supporting narrative.

Conformance to Requirements - All work products shall satisfy the requirements of the work request. The product shall adhere to CBP SDLC-based templates, standards and directives.

File Editing - All text and diagrammatic files shall be editable by the Government.

Format - Work products shall be submitted in media defined in Section 4 Deliverables. The work product format may change from subtask to subtask. Hard copy formats shall follow CBP/DHS Directives and shall be consistent with similar efforts.

Timeliness - Work products shall be submitted on or before the due date specified in the Work Request or submitted in accordance with a later scheduled date determined by the Government.

9.0 PERSONNEL SECURITY

All personnel employed by the contractor or responsible to the contractor for the performance of work hereunder shall either currently possess or be able to favorably pass a full-field background investigation (BI) required by CBP policies and procedures for employment prior to beginning work with CBP. Personnel supporting CLASSIFIED and COMSEC tasks shall also possess or shall be able to obtain a Top Secret clearance with Sensitive Compartmented Information (SCI). This policy applies to any new personnel hired as replacement(s) during the term of this contract.

The contractor shall submit within ten (10) working days after award a list containing the full name, social security number, and date of birth of those people who shall require

background investigation by CBP, and submit such information and documentation as may be required by the Government to have a BI performed. The information provided must be correct and reviewed by the contractor for completeness. This policy also applies to any personnel hired as replacements during the term of the contract. The information must be correct and reviewed by the designated CBP Security Official for completeness. Normally, information requested for a background investigation consists of SF-85P, "Questionnaire for Public Trust Positions", FD-258, "Fingerprint Chart", Criminal History Form, Declaration of Federal Employment Form, ADP Clearance Application Form, Consumer/Credit Report Form and a Financial Statement. Failure of any contract personnel to successfully pass a background investigation shall be cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate as determined and approved by the Contracting Officer/COTR. This policy also applies to any personnel hired as replacements during the term of the contract order.

In addition to a personnel full-field BI, the contractor shall submit a DD 254 for those employees that require additional background information needed to authorize access to National Security Information. New hires or substitutions of personnel are subject to the CBP BI clearance requirements.

All BI forms must be delivered to the CBP, Office of Information & Technology (OIT), Personnel Security Branch, Workforce Management Group (WMG) before the employee can work on this contract. After WMG reviews and accepts the BI package, they forward it to Internal Affairs (IA) for determination of suitability. Until IA initiates a full-field BI and the contractor employee passes the TECS/NCIC/Credit Check, he/she will not be issued a badge, must be escorted at all times while on CBP premises, and will not have access to any CBP systems or sensitive information. If the contractor employee passes the initial TECS/NCIC/Credit checks, he/she is granted a "LIMITED" BI, which enables the employee to have a badge and restricted access to sensitive information. With the "LIMITED" he/she no longer requires an escort.

If the contractor employee fails the TECS/NCIC/Credit checks, his/her BI is put into a "DELAY" status and he/she will not be granted any additional access until the full-field BI is completed. If the contractor employee is put into this "DELAY" status, he/she will not be allowed to work on or bill to this contract until the full-field BI has been successfully adjudicated.

WMG estimates that the TECS/NCIC/Credit check procedures may take one (1) month or longer from the time the packet is received. Completion of the full-field BI may take at additional 90 days or more.

The contractor shall notify the COTR and CBP Office of Information and Technology (OIT) Workforce Management Group (WMG), BI Coordinator of any changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and reassignments including those to another contract. The Contractor/Project Manager is responsible for the completion and

timely submission to the COTR of the CF-242 for all departing contract personnel. The Contractor shall provide OIT/WMG/BI Coordinator the following information on behalf of their contract personnel to telephone number 703-921-6237 or fax the below information to 703-921-6780.

The contractor shall notify the CBP OIT WMG of any change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, and terminations. The contractor shall provide the following information to OIT WMG at Tel. (703) 921-6237 and FAX (703) 921-6780:

Full Name
Social Security Number
Effective Date
Reason for Change

In accordance with Customs Directive No. 51715-006, "Separation Procedures for Contractor Employees (CF-242)", the Contractor is responsible for ensuring that contract employees separating from the agency complete the relevant portions of the CF-242. This requirement covers all Contact employees who depart while the contract is still active (including resignations, termination, etc) or upon final completion of contracts. Failure of a contract to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

"All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, *Information Technology Systems Security Program* and *4300A Sensitive Systems Handbook."*

3052.204-70 Security Requirements For Unclassified Information Technology Resources (JUN 2006)

The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

Within ten (10) days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

The Contractor's IT Security Plan shall comply with Federal laws that include, but are not

limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

Examples of tasks that require security provisions include--

- Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
- Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

CONTRACTOR EMPLOYEE ACCESS

Sensitive Information, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the

applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

- Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of S SI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
- Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
- Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

The Contractor shall include the substance of this clause in all subcontracts at any tier

where the subcontractor may have access to Government facilities, sensitive information, or resources.

Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

- The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
- There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
- The waiver must be in the best interest of the Government.

Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

SECURITY CERTIFICATION/ACCREDITATION

CBP shall provide personnel with the appropriate clearance levels to support the security

certification/accreditation processes under this Agreement in accordance with Attachment D of the DHS Sensitive Systems Handbook Publication 4300A. During all SDLC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools.

SECURITY REVIEW AND REPORTING

- The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.
- The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the Office of Inspector General, CBP ISSM, and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

10.0 POINTS OF CONTACT

Contract deliverables shall be provided to the following specific points of contact:

CBP, COTR
Bureau of Customs and Border Protection
7451 Boston Boulevard, (b)(6), (b)(7)(C)
Springfield, Virginia 22153
Attn: (b) (6)

The On-site Technical Managers for STP (OTM) (Government Team Leads) will manage the technical aspects of the Task Order by measuring the effectiveness of the Task Order by reviewing the deliverables and consistent quality assurance reviews of the contractor's work products are listed below:

(b) (6), (b)(6), (b)(7)(C)
(b) (6), (b)(6), (b)(7)(C)
(b) (6), (b)(6), (b)(7)(C)
(b) (6), (b)(6), (b)(7)(C)
(b) (6), (b)(6), (b)(7)(C)

Issues that could change the terms and conditions of the Task Order will be forwarded by the COTR to the Contracting Officer for action.